REMARKS

The present amendment is in response to the Office Action dated January 22, 2008. Claims 1-5, 7-14, 23-30, and 32-48 are now present in this case. Claims 1, 3, 23, 30, and 32 are amended. Claims 36 are canceled. New claims 44-48 have been added.

The applicant thanks the examiner for the telephonic interview the applicant's attorneys on May 20, 2008. The applicant has amended the claims in light of the Examiner's comments.

Rejections under § 102(e) – Lavian

Claims 1, 7-10, 14, 23, 27-30, and 32-35 stand rejected under 35 U.S.C. § 102(e), as being anticipated by U.S. Patent No. 6,842,781 to Lavian et al. The applicant respectfully traverses this rejection and request reconsideration.

Claim 1

The applicant believes that claim 1 is allowable over the cited reference because the cited reference does not teach at least one element of claim 1, specifically:

> "receiving a request from a central server at a software agent program installed on one of a plurality of remote computers to initiate an intrusion detection service, wherein the request is issued by the central server in response to a notification of a network intrusion, wherein the intrusion detection software includes a stop condition indicating when to stop executing the intrusion detection software, wherein the stop condition includes a condition that no intrusion has been detected for a period of time;"

The Office Action finds this element disclosed by Lavian, based on the finding that Lavian teaches method that includes "receiving request from the NMS [Network Monitoring Server] at a software agent installed on each of a plurality of network devices to load a set of operations associated with a particular task on each respective one of the one or more network devices…wherein the request issued by the central server in response to a notification of inactivity on the network or the network

traffic increases beyond a particular threshold..." and based on interpreting notification of network traffic changes as notification of network intrusion. (Office Action, page 5.) The applicant respectfully disagrees. Lavian does not teach the request was in response activity levels on the network or notification thereof. Lavian teaches "the NMS requests that a network device load a set of operations associated with a particular task." (Lavian Column 7, Lines 43-45.) However, Lavian does not teach what triggers the NMS to make this request. The stated objective of Lavian is to reduce processing load on the NMS "so that it can process more critical tasks." (Lavian, Column 3, Lines 32-33.) Lavian never suggests an objective of reducing network traffic levels. Lavian does mention monitoring of network traffic levels, but only as an example of one task that can be delegated from the NMS to a network device so as to free up the NMS processing resources. (Lavian, Column 3, Lines 34-39, Column 8, Lines 1-6.) That is, Lavian describes network traffic monitoring as an example of software that is downloaded from the central Network Management System (NMS) to a network device. The Office Action cites this traffic monitoring operation as equivalent to the intrusion detection event in the present application. This cannot be viewed as equivalent under 35 U.S.C. §102(e) because the traffic monitor application cannot serve as both the triggering event (i.e., the event that causes network intrusion software to be downloaded) and the software downloaded as a result of the triggering event.

Additionally, Lavian does not teach any stop condition indicating when to stop executing the application, much less a stop condition that includes "when no intrusion has been detected for a period of time."

For at least these reasons, the applicant believes this rejection has been overcome.

Claims 7-10 and 14

Claims 7-10 and 14 are dependent on Claim 1. The applicant believes the rejections of these claims is overcome for at least the same reasons as given above regarding the rejection of claim 1.

Claim 23

Claim 23 has been amended. The applicant believes that claim 23 as amended is allowable over the cited reference because the cited reference does not teach at least one element of claim 23, specifically:

> "an intrusion detection server configured to send a request to install and execute intrusion detection software to software agents at the plurality of the computers when intrusion detection services are needed based on the at least one rule stored in said database, wherein the rule includes a stop condition indicating when to stop executing the intrusion detection software, wherein the stop condition includes a condition that no intrusion has been detected for a period of time."

Lavian teaches "the NMS requests that a network device load a set of operations associated with a particular task," and further teaches that the network devices loads and executes an application capable of performing the set of operations. (Lavian Column 7, Lines 43-45.) However, Lavian does not teach any stop condition indicating when to stop executing the application, much less a stop condition that includes "when no intrusion has been detected for a period of time." For at least these reasons, the applicant believes this rejection of claim 23 has been overcome.

Claims 27-29

Claims 27-29 are dependent on Claim 23. The applicant believes the rejections of these claims is overcome for at least the same reasons as given above regarding the rejection of claim 23.

Claim 30

The applicant believes that claim 30 is allowable over the cited reference because the cited reference does not teach at least one element of claim 30, specifically:

> "transmitting an intrusion detection software installation request from the central server to a plurality of remote computers in response to the notification;"

As discussed above regarding the rejection of claim 1, Lavian does not teach or suggest the request was in response activity levels on the network or notification thereof. Additionally, Lavian does not teach any stop condition indicating when to stop executing the application, much less a stop condition that includes "when no intrusion has been detected for a period of time." For at least these reasons, the applicant believes this rejection has been overcome.

Claims 32-35

Claims 32-35 are dependent on Claim 30. The applicant believes the rejections of these claims is overcome for at least the same reasons as given above regarding the rejection of claim 30.

Rejections under § 103(a) – Lavian / Jansen

Claims 2-4, 11, 13, 24-26, 36, and 38 stand rejected under 35 U.S.C. § 103(a) as unpatentable by U.S. Patent No. 6,842,781 to Lavian et al. combined with Non-Patent Literature "Applying Mobile Agents to Intrusion Detection Response", pages 1-46 by Jansen et al. The applicant respectfully traverses this rejection and request reconsideration.

Claims 2-4, 11 and 13

The Office Action finds Lavian teaches the elements of claim 1 and finds Jansen teaches the elements added by claims 2-4, 11 and 13. The inapplicability of Lavian with respect to claim 1 has already been discussed above. The addition of Jansen does not cure this deficiency. Jansen teaches mobile agents for intrusion detection and response. Jansen discloses "gracefully terminating" a mobile agent if the agent is producing too many false positives or is an older version. (Jansen 3.1.5.) However, the combination of Lavian and Jansen does not teach a stop condition that includes "when no intrusion has been detected for a period of time." For at least these reasons, the applicant believes these rejections have been overcome.

Claims 24-26

The Office Action finds Lavian teaches the elements of claim 23 and finds Jansen teaches the elements added by claims 24-26. The inapplicability of Lavian with respect to claim 23 has already been discussed above The addition of Jansen does not cure this deficiency. Jansen teaches mobile agents for intrusion detection and response. Jansen discloses "gracefully terminating" a mobile agent if the agent is producing too many false positives or is an older version. (Jansen 3.1.5.) However, the combination of Lavian and Jansen does not teach a stop condition that includes "when no intrusion has been detected for a period of time." For at least these reasons, the applicant believes these rejections have been overcome.

Claims 36 and 38

Claim 36 has been canceled as the element it recited has been moved to independent claim 30. The Office Action finds Lavian teaches the elements of claim 30 and finds Jansen teaches the elements added by claims 36-38. The addition of Jansen does not cure this deficiency. Jansen teaches mobile agents for intrusion detection and response. Jansen discloses "gracefully terminating" a mobile agent if the agent is producing too many false positives or is an older version. (Jansen 3.1.5.) However, the combination of Lavian and Jansen does not teach a stop condition that includes "when no intrusion has been detected for a period of time." For at least these reasons, the applicant believes these rejections have been overcome.

Rejections under § 103(a) – Lavian / Jansen / Sprunk

Claims 5, 12, 37, and 41-43 stand rejected under 35 U.S.C. § 103(a) as unpatentable by U.S. Patent No. 6,842,781 to Lavian et al. combined with Non-Patent Literature "Applying Mobile Agents to Intrusion Detection Response", pages 1-46 by Jansen et al., and combined with U.S. Patent Publication 2002/0003884 to Sprunk. The applicant respectfully traverses this rejection and request reconsideration.

Claims 5, 12, 37, and 41-43

Claims 5, 12, 37, 41, 42 and 43 are dependent on claims 2 ,11, 36, 11, 2 and 2, respectively. The Office Action finds the combination of Lavian and Jansen

teaches the elements of claim 2, 11 and 36 and finds Sprunk teaches the elements added by claims 5, 12, 37, 41, 42 and 43. The inapplicability of the combination of Lavian and Jansen with respect to claims 2, 11 and 36 has already been discussed above. The addition of Sprunk does not cure this deficiency. Sprunk teaches a method of information authentication using an access control processor that stops execution of applications if an error is detected or if authorization expires. (Sprunk, paragraph [0054].) However, the combination of Lavian, Jansen and Sprunk does not teach a stop condition that includes "when no intrusion has been detected for a period of time." For at least these reasons, the applicant believes these rejections have been overcome.

Rejections under § 103(a) – Lavian / Brown

Claims 39-40 stand rejected under 35 U.S.C. § 103(a) as unpatentable by U.S. Patent No. 6,842,781 to Lavian et al. combined with U.S. Patent No. 6,401,238 to Brown et al. The applicant respectfully traverses this rejection and request reconsideration.

Claims 39-40

The Office Action finds Lavian teaches the elements of claim 1 and finds Brown teaches the elements added by claims 39-40. The inapplicability of Lavian with respect to claim 1 has already been discussed above. The addition of Brown does not cure this deficiency. Brown teaches a method of deploying applications to client computers in a network, selecting different versions of an application depending on user needs and current network conditions. (Brown, Column 1, Lines 37-45.) However, the combination of Lavian and Brown does not teach a stop condition that includes "when no intrusion has been detected for a period of time." For at least these reasons, the applicant believes these rejections have been overcome.

Patentability of new claims

New claims 44-48

The applicant believes claim 44 is patentable over the cited references because it recites at least one element not taught or suggested by the cited references. Specifically, claim 44 recites

> "sending a message to the selected computer to cease execution of the intrusion detection software when a stop condition is detected, wherein the stop condition includes a condition that no intrusion has been detected for a period of time."

As discussed above all the cited references do not teach, alone or in combination, a stop condition that includes "when no intrusion has been detected for a period of time." For at least this reason, the applicant believes claim 44 is patentable. Claims 45 and 47 are dependent on claim 44. The applicant believes these claims are patentable for at least the same reasons as given for claim 44.

Conclusion

In view of the above amendments and remarks, reconsideration of the subject application and its allowance are kindly requested. The applicant has made a good faith effort to place all claims in condition for allowance. If questions remain regarding the present application, the Examiner is invited to contact the undersigned at (206) 757-8029.

Respectfully submitted,
Arturo Maria
Davis Wright Tremaine LLP

/Michael J. Donohue, Reg. #35,859/

Michael J. Donohue

1201 Third Avenue
Suite 2200
Seattle, Washington 98101
Phone: (206) 757-8029
Fax: (206) 757-7029

11166918_1.DOC